Representing integers by multilinear polynomials

Lenny Fukshansky
Claremont McKenna College

Diophantine Analysis Online Seminar
Moscow State University
April 8, 2021

Representation problems

Let $F(\boldsymbol{x})$ be a polynomial in n variables with integer coefficients and b be an integer.

Representation problems

Let $F(\boldsymbol{x})$ be a polynomial in n variables with integer coefficients and b be an integer.

Problem 1

Determine if the equation $F(\boldsymbol{x}) = b$ has integer solutions. In other words, is b **representable** *by F over $\mathbb{Z}$?*

Representation problems

Let $F(\boldsymbol{x})$ be a polynomial in n variables with integer coefficients and b be an integer.

Problem 1

Determine if the equation $F(\boldsymbol{x}) = b$ has integer solutions. In other words, is b **representable** *by F over $\mathbb{Z}$?*

Problem 2

Provided $F(\boldsymbol{x}) = b$, find a solution of bounded size. In other words find $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$ and

$$|\boldsymbol{a}| \leq S(F)$$

for an appropriate function $S(F)$ of the coefficients of F, where $|\boldsymbol{a}|$ is the sup-norm of $\boldsymbol{a}$.

Hilbert's 10th problem

In general, these are hard problems: Hilbert's 10th problem asks whether there is an algorithm that would take F and b on the input and decide whether an integer solution exists.

Hilbert's 10th problem

In general, these are hard problems: Hilbert's 10th problem asks whether there is an algorithm that would take F and b on the input and decide whether an integer solution exists.

In his breakthrough 1970 work, **Yuri Matiyasevich** showed undecidability of Hibert's 10th problem, i.e. such an algorithm cannot in general exist.

Hilbert's 10th problem

In general, these are hard problems: Hilbert's 10th problem asks whether there is an algorithm that would take F and b on the input and decide whether an integer solution exists.

In his breakthrough 1970 work, **Yuri Matiyasevich** showed undecidability of Hibert's 10th problem, i.e. such an algorithm cannot in general exist.

An algorithm, however, exists for some special classes of polynomials. One way to describe such an algorithm is in terms of a search bound.

Search bounds

Suppose it is possible to prove a theorem like this:

If a polynomial equation

$$F(\boldsymbol{x}) = b$$

has a solution $\boldsymbol{a} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ *then it has such a solution with* $|\boldsymbol{a}|$ *bounded by some function of the coefficients of* F *and* b*, call it* $S(F, b)$.

Search bounds

Suppose it is possible to prove a theorem like this:

If a polynomial equation

$$F(\boldsymbol{x}) = b$$

has a solution $\boldsymbol{a} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ *then it has such a solution with* $|\boldsymbol{a}|$ *bounded by some function of the coefficients of* F *and* b*, call it* $S(F, b)$*.*

Then deciding whether $F(\boldsymbol{x}) = b$ has a solution reduces to a finite search algorithm. Hence $S(F, b)$ can be referred to as a **search bound**. Search bounds can be used to check if a solution exists and to find it in case it does.

Existence of search bounds

Due to Matiyasevich's negative result, search bounds cannot exist in general, but they are known to exist for some classes of polynomials:

Existence of search bounds

Due to Matiyasevich's negative result, search bounds cannot exist in general, but they are known to exist for some classes of polynomials:

- Linear forms and equations (Siegel's lemma and generalizations)

Existence of search bounds

Due to Matiyasevich's negative result, search bounds cannot exist in general, but they are known to exist for some classes of polynomials:

- Linear forms and equations (Siegel's lemma and generalizations)
- Quadratic forms and equations (Cassels' theorem and generalizations)

Existence of search bounds

Due to Matiyasevich's negative result, search bounds cannot exist in general, but they are known to exist for some classes of polynomials:

- Linear forms and equations (Siegel's lemma and generalizations)
- Quadratic forms and equations (Cassels' theorem and generalizations)
- Cubic forms in ≥ 17 variables satisfying some additional technical conditions (Browning–Dietmann–Elliott, 2012)

Existence of search bounds

Due to Matiyasevich's negative result, search bounds cannot exist in general, but they are known to exist for some classes of polynomials:

- Linear forms and equations (Siegel's lemma and generalizations)
- Quadratic forms and equations (Cassels' theorem and generalizations)
- Cubic forms in ≥ 17 variables satisfying some additional technical conditions (Browning–Dietmann–Elliott, 2012)

In fact, there have also been some recent results for higher degree polynomial systems satisfying certain additional technical non-singularity conditions.

Universal polynomials

A polynomial $F(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ that represents every $b \in \mathbb{Z}$ is called **universal**. Examples of universal polynomials include:

- Linear forms with relatively prime coefficients

Universal polynomials

A polynomial $F(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ that represents every $b \in \mathbb{Z}$ is called **universal**. Examples of universal polynomials include:

- Linear forms with relatively prime coefficients
- Sum of ≥ 4 squares (Lagrange's theorem)

Universal polynomials

A polynomial $F(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ that represents every $b \in \mathbb{Z}$ is called **universal**. Examples of universal polynomials include:

- Linear forms with relatively prime coefficients
- Sum of ≥ 4 squares (Lagrange's theorem)

Universality of quadratic forms has been studied extensively by multiple authors since the work of Lagrange, Legendre and Gauss, culminating in the classical Hasse-Minkowski theorem.

Universal polynomials

A polynomial $F(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ that represents every $b \in \mathbb{Z}$ is called **universal**. Examples of universal polynomials include:

- Linear forms with relatively prime coefficients
- Sum of ≥ 4 squares (Lagrange's theorem)

Universality of quadratic forms has been studied extensively by multiple authors since the work of Lagrange, Legendre and Gauss, culminating in the classical Hasse-Minkowski theorem.

More recently, there were such celebrated criteria for universality as 15 (Conway–Schneeberger) and 290 (Bhargava–Hanke) theorems for classically integral and integral positive definite forms, respectively.

Universal polynomials

A polynomial $F(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ that represents every $b \in \mathbb{Z}$ is called **universal**. Examples of universal polynomials include:

- Linear forms with relatively prime coefficients
- Sum of ≥ 4 squares (Lagrange's theorem)

Universality of quadratic forms has been studied extensively by multiple authors since the work of Lagrange, Legendre and Gauss, culminating in the classical Hasse-Minkowski theorem.

More recently, there were such celebrated criteria for universality as 15 (Conway–Schneeberger) and 290 (Bhargava–Hanke) theorems for classically integral and integral positive definite forms, respectively.

In this talk, we want to discuss universality of multilinear integral forms of arbitrary degree.

Multilinear forms

For integers $1 \leq d \leq n$, define

$$[n] := \{1, \ldots, n\}, \ \mathcal{I}_d(n) := \{I \subseteq [n] : |I| = d\}.$$

For each indexing set $I = \{i_1, \ldots, i_d\} \in \mathcal{I}_d(n)$ with

$$1 \leq i_1 < \cdots < i_d \leq n,$$

define the monomial x_I in variables $x_{i_1}, \ldots, x_{i_d}$ out of $x_1, \ldots, x_n$ as

$$x_I := x_{i_1} \cdots x_{i_d}.$$

Multilinear forms

For integers $1 \leq d \leq n$, define

$$[n] := \{1, \ldots, n\}, \ \mathcal{I}_d(n) := \{I \subseteq [n] : |I| = d\}.$$

For each indexing set $I = \{i_1, \ldots, i_d\} \in \mathcal{I}_d(n)$ with

$$1 \leq i_1 < \cdots < i_d \leq n,$$

define the monomial x_I in variables $x_{i_1}, \ldots, x_{i_d}$ out of $x_1, \ldots, x_n$ as

$$x_I := x_{i_1} \cdots x_{i_d}.$$

An **integer multilinear** (n, d)**-form** is a polynomial of the form

$$F(x_1, \ldots, x_n) = \sum_{I \in \mathcal{I}_d(n)} f_I x_I \in \mathbb{Z}[x_1, \ldots, x_n].$$

This is a homogeneous polynomial in n variables of degree d which has degree 1 in each of the variables.

Multilinear forms representing integers

We say that F **represents** an integer b it there exists an integer vector $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$.

Multilinear forms representing integers

We say that F **represents** an integer b it there exists an integer vector $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$.

Question 1

Under what conditions on F does such a polynomial represent all integers?

Multilinear forms representing integers

We say that F **represents** an integer b it there exists an integer vector $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$.

Question 1

Under what conditions on F does such a polynomial represent all integers?

The first observation is that coefficients f_I of F must be relatively prime: if $g = \gcd(f_I)_{I \in \mathcal{I}_d(n)} > 1$, then g must divide $F(\boldsymbol{a})$ for every $\boldsymbol{a} \in \mathbb{Z}^n$, and hence an integer b that is not a multiple of g is not represented by F. We say that F **is coprime** if $\gcd(f_I)_{I \in \mathcal{I}_d(n)} = 1$.

Multilinear forms representing integers

We say that F **represents** an integer b it there exists an integer vector $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$.

Question 1

Under what conditions on F does such a polynomial represent all integers?

The first observation is that coefficients f_I of F must be relatively prime: if $g = \gcd(f_I)_{I \in \mathcal{I}_d(n)} > 1$, then g must divide $F(\boldsymbol{a})$ for every $\boldsymbol{a} \in \mathbb{Z}^n$, and hence an integer b that is not a multiple of g is not represented by F. We say that F **is coprime** if $\gcd(f_I)_{I \in \mathcal{I}_d(n)} = 1$.

Hence F being coprime is a necessary condition for F to be universal. Our first result demonstrates some sufficient conditions.

Effective representation result - I

In fact, we produce an *effective* theorem: not only do we prove existence of representations, we give a bound on their size.

Theorem 1 (A. Böttcher, L.F. - 2019)

Let $F(\boldsymbol{x})$ be a coprime integer multilinear (n, d)-form. Suppose in addition that at least one of the following two conditions holds:

(a) *The nonzero coefficients of F are pairwise coprime,*

(b) *$n = d + 1$ and F has a pair of coprime coefficients.*

Then F represents all integers. Further, for each $b \in \mathbb{Z}$ there exists an $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$ and

$$|\boldsymbol{a}| \leq |b| \, (2|F|)^{d! \, \mathrm{e}} \, ,$$

where $|\boldsymbol{a}| = \max_{1 \leq i \leq n} |a_i|$, $|F| = \max_{I \in \mathcal{I}_d(n)} |f_I|$, and $\mathrm{e} = 2.71828\ldots$.

Proof idea: separation of variables

To prove Theorem 1, we argue by induction on $\ell \geq 1$, the number of monomials of F. The heart of the matter is the situation when every variable is present in $\ell - 1$ monomials. Then each monomial depends on $\leq n-1$ variables, and so $d \leq n-1$. Hence

$$F(\boldsymbol{x}) = x_1 G(x_2, \ldots, x_n) + f_I \prod_{i=2}^{n} x_i,$$

where $I = \{2, \ldots, n\}$ and G is a homogeneous polynomial of degree $d-1$ linear in each of the $n-1$ variables with integer pairwise relatively prime coefficients. By induction hypothesis, there exists a vector $\boldsymbol{a}' \in \mathbb{Z}^{n-1}$ with bounded sup-norm such that $G(\boldsymbol{a}') = 1$. Then

$$F\left(\left(b - f_I \prod_{i=2}^{n} a'_i\right),\ \boldsymbol{a}'\right) = \left(b - f_I \prod_{i=2}^{n} a'_i\right) G(\boldsymbol{a}') + f_I \prod_{i=2}^{n} a'_i = b.$$

Sparse representations

As a consequence of Theorem 1, we can also produce sparse representations for integers by multilinear forms: we say that an integer b is represented by F k-**sparsely** if there exists a nonzero vector $\boldsymbol{a} \in \mathbb{Z}^n$ with no more than k nonzero coordinates such that $F(\boldsymbol{a}) = b$.

Sparse representations

As a consequence of Theorem 1, we can also produce sparse representations for integers by multilinear forms: we say that an integer b is represented by F k-**sparsely** if there exists a nonzero vector $\boldsymbol{a} \in \mathbb{Z}^n$ with no more than k nonzero coordinates such that $F(\boldsymbol{a}) = b$.

Corollary 2

If some coefficient of F is equal to ± 1, then F represents b by a d-sparse vector $\boldsymbol{a} \in \mathbb{Z}^n$ with one coordinate equal to $\pm b$ and the rest of the nonzero coordinates equal to 1. Otherwise, if F has all nonzero pairwise coprime coefficients, then F represents every integer k-sparsely if and only if $k \geq d + 1$. If this is the case, then for every $b \in \mathbb{Z}$ there exists a k-sparse vector $\boldsymbol{z} \in \mathbb{Z}^n$ such that $F(\boldsymbol{z}) = 0$ and

$$|\boldsymbol{z}| \leq |b| \left(2|F|\right)^{d!e}.$$

Effective representation result - II

We remark that neither (a) nor (b) in Theorem 1 is a necessary condition. For example, a coprime integer linear $(n, 1)$-form

$$F(\boldsymbol{x}) = f_1x_1 + \cdots + f_nx_n$$

represents all integers even if no pair of coefficients is coprime, and there are $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$ and $|\boldsymbol{a}| \leq |b|$.

Effective representation result - II

We remark that neither (a) nor (b) in Theorem 1 is a necessary condition. For example, a coprime integer linear $(n, 1)$-form

$$F(\boldsymbol{x}) = f_1 x_1 + \cdots + f_n x_n$$

represents all integers even if no pair of coefficients is coprime, and there are $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$ and $|\boldsymbol{a}| \leq |b|$.

To give another example, the coprime $(3, 2)$-form

$$F(x, y, z) = 6xy + 10xz + 15yz$$

represents every integer although the gcd of each pair of coefficients is greater than 1.

Effective representation result - II

We remark that neither (a) nor (b) in Theorem 1 is a necessary condition. For example, a coprime integer linear $(n, 1)$-form

$$F(\boldsymbol{x}) = f_1 x_1 + \cdots + f_n x_n$$

represents all integers even if no pair of coefficients is coprime, and there are $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$ and $|\boldsymbol{a}| \leq |b|$.

To give another example, the coprime $(3, 2)$-form

$$F(x, y, z) = 6xy + 10xz + 15yz$$

represents every integer although the gcd of each pair of coefficients is greater than 1. This is the case $p = 5$ of the following observation.

Proposition 3 (A. Böttcher, L.F. - 2019)

If $p \geq 5$ is an integer and neither 2 nor 3 divides p, then the polynomial $F(x, y, z) = 6xy + 2pxz + 3pyz$ represents every integer.

Determinantal forms

For a special class of forms we have an "if and only if" result.

Proposition 4 (A. Böttcher, L.F. - 2019)

Let $A = (a_{ij}) \in \mathbb{Z}^{n \times s}$ *with* $1 \leq s < n$ *and consider the integer multilinear* $(n(n-s), n-s)$*-form*

$$F(\boldsymbol{y}) = \det \begin{pmatrix} a_{11} & \dots & a_{1s} & y_{11} & \dots & y_{1(n-s)} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{ns} & y_{n1} & \dots & y_{n(n-s)} \end{pmatrix}.$$

F *represents all integers if and only if the minors of* A *are coprime. If so, then there is a* $\boldsymbol{y} \in \mathbb{Z}^{n(n-s)}$ *such that* $F(\boldsymbol{y}) = b$ *and*

$$|\boldsymbol{y}| \leq n^2 |b||A|((n-1)!D^n + 2)^{n-1},$$

where $D =$ *minimum of absolute values of nonzero minors of* A.

Extending a matrix

The underlying principle behind the previous observation is the following classical arithmetic result:

For integers $1 \le m < n$, an $n \times m$ integer matrix A can be extended to a matrix in $\mathrm{GL}_n(\mathbb{Z})$ if and only if the $m \times m$ minors of A are relatively prime.

Extending a matrix

The underlying principle behind the previous observation is the following classical arithmetic result:

For integers $1 \leq m < n$, an $n \times m$ integer matrix A can be extended to a matrix in $\mathrm{GL}_n(\mathbb{Z})$ if and only if the $m \times m$ minors of A are relatively prime.

Such a matrix A is extendable to a matrix in $\mathrm{GL}_n(\mathbb{Z})$ if and only if its columns form a **primitive collection** of vectors, i.e. extendable to a basis for $\mathbb{Z}^n$. If there is one such extension, there are infinitely many.

Extending a matrix

The underlying principle behind the previous observation is the following classical arithmetic result:

For integers $1 \leq m < n$, an $n \times m$ integer matrix A can be extended to a matrix in $\mathrm{GL}_n(\mathbb{Z})$ if and only if the $m \times m$ minors of A are relatively prime.

Such a matrix A is extendable to a matrix in $\mathrm{GL}_n(\mathbb{Z})$ if and only if its columns form a **primitive collection** of vectors, i.e. extendable to a basis for $\mathbb{Z}^n$. If there is one such extension, there are infinitely many.

Question 2

If $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m \in \mathbb{Z}^n$ is a primitive collection, then how many collections $\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m} \in \mathbb{Z}^n$ there exist so that

$$\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m}$$

is a basis for $\mathbb{Z}^n$, $|\boldsymbol{b}_i| \leq T \ \forall\ 1 \leq i \leq n-m$ as $T \to \infty$?

Counting basis extensions - I

Theorem 5 (M. Forst, L.F. - 2020)

Let $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}^n$ be a primitive collection of vectors.

1. *If $m < n-1$, the number of vectors $\mathbf{b} \in \mathbb{Z}^n$ with $|\mathbf{b}| \leq T$ such that the collection $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}$ is again primitive is equal to $\Theta(T^n)$ as $T \to \infty$.*
2. *If $m = n-1$, the number of vectors $\mathbf{b} \in \mathbb{Z}^n$ with $|\mathbf{b}| \leq T$ such that the collection $\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}$ is a basis for $\mathbb{Z}^n$ is equal to $\Theta(T^{n-1})$ as $T \to \infty$.*

As a result, for any $1 \leq k < n-m$ there exist $\Theta(T^{nk})$ collections of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathbb{Z}^n$ with $|\mathbf{b}_i| \leq T$, $1 \leq i \leq k$, such that $\{\mathbf{a}_i, \mathbf{b}_j : 1 \leq i \leq m, 1 \leq j \leq k\}$ is again primitive. Further, there are $\Theta(T^{n^2-nm-1})$ such collections $\mathbf{b}_1, \ldots, \mathbf{b}_{n-m}$ so that

$$\mathbb{Z}^n = \operatorname{span}_{\mathbb{Z}} \{\mathbf{a}_1, \ldots, \mathbf{a}_m, \mathbf{b}_1, \ldots, \mathbf{b}_{n-m}\}.$$

Proof outline: adding one vector

Lemma 6

Let $1 \leq m < n-1$ *and let* $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in \mathbb{Z}^n$ *be a primitive collection of vectors. For* $T > 0$, *define*

$$f(T) = \left|\{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{x} \text{ is primitive}, |\boldsymbol{x}| \leq T\}\right|,$$

then as $T \to \infty$, (Cesáro, 1884)

$$f(T) \leq \left(\zeta(n)^{-1} + \varepsilon\right)(2T+1)^n, \tag{1}$$

where ζ *is the Riemann zeta-function,* $\varepsilon > 0$. *Additionally,*

$$f(T) \geq \beta(n, m, A)\, T^n, \tag{2}$$

where $\beta(n, m, A)$ *is a constant depending only on* n, m *and the matrix* A.

Proof outline: adding last vector

Lemma 7

For $n \geq 2$, let $\boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1} \in \mathbb{Z}^n$ a primitive collection of vectors and $A = (\boldsymbol{a}_1 \ \dots \ \boldsymbol{a}_{n-1})$ the corresponding $n \times (n-1)$ matrix. For each $1 \leq k \leq n$, let A_k be the $(n-1) \times (n-1)$ submatrix of A obtained by deleting k-th row, and define

$$\Delta_A := \max\{|\det(A_k)| : 1 \leq k \leq n\}.$$

Define also

$$f(T) = \left|\{\boldsymbol{z} \in \mathbb{Z}^n : \mathbb{Z}^n = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}, \boldsymbol{z}\}, |\boldsymbol{z}| \leq T\}\right|,$$

then

$$f(T) \sim 2\left(\frac{(2T)^{n-1}}{\Delta_A}\right)$$

as $T \to \infty$.

Counting basis extensions - II

Any lattice $\Lambda \subset \mathbb{R}^n$ is of the form $\Lambda = U\mathbb{Z}^n$ for some matrix $U \in \mathrm{GL}_n(\mathbb{R})$. As such, bases in Λ are in bijective correspondence with bases in $\mathbb{Z}^n$, given by multiplication by U. This correspondence allows to extend Theorem 5 to arbitrary lattices, where we call a collection of vectors in Λ primitive if it is a basis or can be extended to a basis of Λ.

Counting basis extensions - II

Any lattice $\Lambda \subset \mathbb{R}^n$ is of the form $\Lambda = U\mathbb{Z}^n$ for some matrix $U \in \mathrm{GL}_n(\mathbb{R})$. As such, bases in Λ are in bijective correspondence with bases in $\mathbb{Z}^n$, given by multiplication by U. This correspondence allows to extend Theorem 5 to arbitrary lattices, where we call a collection of vectors in Λ primitive if it is a basis or can be extended to a basis of Λ.

Corollary 8

Let $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$ be a primitive collection of vectors in a full-rank lattice $\Lambda \subset \mathbb{R}^n$ with $1 \leq m < n$. Then there are $\Theta(T^{n^2-nm-1})$ collections of vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m} \in \Lambda$ such that $|\boldsymbol{b}_i| \leq T$ for each $1 \leq i \leq n-m$ and

$$\Lambda = \mathrm{span}_{\mathbb{Z}} \{\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n-m}\}.$$

Two dimensions: the Farey fractions connection

Recall that for each $n \geq 1$, the *Farey series of order n*, denoted $\mathcal{F}_n$, is the set of all rationals $a/b \in [0,1]$ with $\gcd(a,b) = 1$ and $b \leq n$ written in ascending order. There is a nice connection between Farey series and bases for $\mathbb{Z}^2$.

Lemma 9

Let $\boldsymbol{x}_1 = (a,b)^\top$ *and* $\boldsymbol{x}_2 = (c,d)^\top$ *be primitive vectors in* $\mathbb{Z}^2$ *with*

$$0 < a < b, \; 0 < c < d,$$

and let $n = \max\{b,d\}$. *Then* $\boldsymbol{x}_1, \boldsymbol{x}_2$ *form a basis for* $\mathbb{Z}^2$ *if and only if* $\frac{a}{b}$ *and* $\frac{c}{d}$ *are consecutive elements in the Farey series* $\mathcal{F}_n$*; we call such elements* **Farey neighbors**.

Two dimensions: the Farey fractions connection

Recall that for each $n \geq 1$, the *Farey series of order n*, denoted $\mathcal{F}_n$, is the set of all rationals $a/b \in [0, 1]$ with $\gcd(a, b) = 1$ and $b \leq n$ written in ascending order. There is a nice connection between Farey series and bases for $\mathbb{Z}^2$.

Lemma 9

Let $\boldsymbol{x}_1 = (a, b)^\top$ and $\boldsymbol{x}_2 = (c, d)^\top$ be primitive vectors in $\mathbb{Z}^2$ with

$$0 < a < b, \; 0 < c < d,$$

and let $n = \max\{b, d\}$. Then $\boldsymbol{x}_1, \boldsymbol{x}_2$ form a basis for $\mathbb{Z}^2$ if and only if $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive elements in the Farey series $\mathcal{F}_n$; we call such elements **Farey neighbors**.

Then Farey neighbors of a fraction a/b correspond to the (positive) basis extensions of the vector $(a, b)^\top$, and their number grows like $2n/b$ as $n \to \infty$, which is consistent with our Lemma 7 in the two-dimensional case.

Open question

In conclusion, I want to mention a remaining open question:

Question 3

Does every multilinear coprime integer form represent all the integers? In other words, is the coprimality condition necessary and **sufficient** *for the form to be universal?*

We do not know of any counter-examples. In fact, we may know of some additional families of multilinear forms for which coprimality condition is sufficient – this is work in progress (joint with Max Forst).

References

A. Böttcher and L. Fukshansky, *Representing integers by multilinear polynomials*, Research in Number Theory, vol. 6 no. 4 (2020), Article #38.

M. Forst and L. Fukshansky, *Counting basis extensions in a lattice*, arXiv:2011.05307

Preprints are available at:

`http://math.cmc.edu/lenny/research.html`

References

A. Böttcher and L. Fukshansky, *Representing integers by multilinear polynomials*, Research in Number Theory, vol. 6 no. 4 (2020), Article #38.

M. Forst and L. Fukshansky, *Counting basis extensions in a lattice*, arXiv:2011.05307

Preprints are available at:

`http://math.cmc.edu/lenny/research.html`

Thank you!